Entorno personal de aprendizaje:

Curso de Ciberseguridad: Seguridad en medios digitales

Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Viceministerio de Tecnologías de la Información y Comunicación

Director General de Inclusión Digital y TIC en la Educación

Dirección General de Ciberseguridad y Protección a la Información

Información

SEDE 1

Dirección: Complejo Santos E2 - Gral. Santos 1170 c/ Concordia
Teléfono: (+595 21) 217 9000
Correo electrónico: comunicacion@mitic.gov.py
Mesa de entrada: sgeneral@mitic.gov.py

Asunción – Paraguay

Entorno personal de aprendizaje (PLE):
Curso de Ciberseguridad: Seguridad en medios digitales

Todas las imágenes presentes en este material de apoyo educativo han sido reconocidas y, en todos los casos, son de uso libre. Todas las fuentes bibliográficas utilizadas en este material de apoyo educativo han son citadas mediante el gestor de referencias bibliográficas Zotero, desarrollado por el Center for History and New Media de la Universidad George Mason, utilizando el estilo de la American Psychological Association Séptima Edición.

Obra publicada con licencia de Creative Commons Reconocimiento-Compartir Igual 4.0

https://creativecommons.org/licenses/by-sa/4.0/

Programa
Ciberseguridad: Seguridad en medios digitales

Introducción

La ciberseguridad se ha convertido en los últimos años en una cuestión que ha generado gran interés en empresas de todo tipo, así como en personas de cualquier parte del mundo apasionadas de las TICs. El imparable desarrollo digital ha convertido en imprescindible la protección de la información para evitar el robo de datos sensibles entre otros peligros en medios digitales.

Saber cómo abordar la seguridad en la red y reaccionar ante las amenazas como a la privacidad en Internet y otros, son desafíos a los que las personas y las empresas se enfrentan casi cada día. De ello depende que en la interacción digital nuestros datos bancarios, proyectos profesionales, documentos confidenciales, y otros estén a salvo de los denominados ciberdelincuentes.

Si ya de por sí nuestra relación con el mundo tecnológico cambia constantemente debido a los avances y las nuevas plataformas, la crisis del coronavirus ha supuesto un punto de inflexión y una forma de comprender lo importante que es incrementar las medidas de seguridad, algo que hemos visto aumentar de forma drástica tras la adaptación forzosa de muchos profesionales al teletrabajo, o de reuniones particulares virtuales, escuelas y colegios virtuales, etc. Los ataques de phishing, suplantación de identidad o ransomware son técnicas habituales que nos aquejan día a día.

1. Identificación

Módulo	Entorno Personal de Aprendizaje (PLE): aprender en línea efectivamente.
Modalidad	Virtual
Carga horaria	60 horas pedagógicas
Profesores	Rodney Colman, Victor Vázquez, Fernando Martínez
Pre-requisitos	Ninguno

El esfuerzo estimado es de 10 (diez) horas por semana, considerando la lectura de los materiales, la visualización de los videos, el desarrollo de las tareas y la participación en los foros, durante las seis semanas de duración del módulo.

2. Descripción

Nos preguntamos: ¿por qué una persona sin conocimientos técnicos debería preocuparse por la seguridad de sus datos? ¿Acaso los profesionales de las áreas TICs no son los únicos responsables de la seguridad? Sin embargo, hay que recordar que el eslabón más débil en la cadena de seguridad de la información es justamente el usuario final: la persona que utiliza la tecnología, que tiene en su poder información valiosa y que, en la mayoría de los casos, no es una persona con conocimientos muy técnicos sobre las TICs.

Cuando una persona o grupo malicioso busca realizar un ataque contra un objetivo (una empresa, una persona, una institución gubernamental, etc.), estudia las maneras de llegar y una de las formas es justamente por el eslabón más débil como punto de entrada. Es por eso que es tan importante que los usuarios conozcan las herramientas y medidas de protección que se desarrollan y las implementen en el día a día para proteger la información tanto en la vida cotidiana profesional como la personal. En una organización no es suficiente que solo los profesionales de las áreas TICs seguricen los sistemas con estas herramientas, es requerido también que los usuarios conozcan y así tomen las medidas de protección correspondientes para protegerse a sí mismo y también a los demás.

3. Justificación

Hoy en día, todas las personas utilizan medios digitales tanto en la vida privada como laboral, por lo que es fundamental que todos conozcan las amenazas a las que se está expuesto, así como las medidas de protección básicas que se deben tener en cuenta al utilizarlas. Para ello ponemos a disposición el curso llamado "Protege tu información - Seguridad en la era de

los medios digitales", un curso no-técnico, orientado a ciudadanos interesados en la protección de su navegación en Internet. Este curso no requiere que el alumno interesado cuente con conocimientos previos de áreas relacionadas a las TICs y no posee ningún otro pre-requisito.

4. Objetivos

4.1. Objetivo general

Adquirir, comprender y/o consolidar las competencias relacionadas a la capacidad de entender en forma básica, la razón de la existencia y del funcionamiento de los ataques cibernéticos, dentro del marco del ciudadano digital, desde donde se genera la necesidad de las medidas de protección para garantizar la convivencia armoniosa de las actividades digitales cotidianas.

4.2. Objetivos específicos

- Comprender los Riesgos y cuidados para la gestión de credenciales.
- Comprender los Peligros y los tipos de Protección en el uso del Correo Electrónico.
- Conocer y poner en práctica las medidas de protección ante las diferentes técnicas de Ingeniería Social.
- Conocer buenas prácticas para la Navegación segura por Internet.
- Conocer las buenas prácticas la protección contra amenazas a los equipos.
- Comprender la necesidad de la protección de datos e información.

5. Competencias

El estudiante comprende la importancia de la protección de datos e información en medios digitales, teniendo en cuenta la importancia de los mismos, y siguiendo las normas establecidas para evitar los riesgos que

implican la navegación en internet, conocer técnicas de ingeniería social, protección en el uso del correo electrónico, y la gestión de credenciales.

6. Contenido

6.1. Control de Acceso – Credenciales

- ¿Qué es la Autenticación?
- Buenas Prácticas de Contraseñas.
- Contraseñas Robustas.
- Autenticación de Doble Factor (A2F).
- Gestores de Contraseñas.

6.2. Correo Electrónico

- Spam o Correo no deseado.
- Enlaces Falsos.
- Remitentes Falsos.
- Phishing a través de Correo Electrónico.
- Buenas Prácticas en el uso del Correo Electrónico.

6.3. Ingeniería Social

- ¿Qué es la Ingeniería Social?
- Principios de la Ingeniería Social.
- Tipos de Ingeniería Social.
- Redes sociales e información personal en Internet.
- Cuidados frente a la Ingeniería Social.

6.4. Navegación Segura

- Riesgos en la Navegación.
- Drive-by Download.
- Protección anti-phishing/anti-malware del navegador.
- Plugins del navegador.
- Complementos de Seguridad.

6.5. Seguridad en Equipos

- Riesgos en los Equipos.
- El Malware.
- Ransomware.
- Vulnerabilidades.
- Actualizaciones.
- Software de Seguridad.

6.6. Protección de los Datos

- Riesgos a la Información.
- Protegiendo la Sesión.
- Encriptación de Datos.
- Copias de Seguridad.
- Borrado Remoto.
- Herramientas de Borrado Remoto.

7. Metodología

El desarrollo teórico práctico de las diferentes sesiones de aprendizaje, mediante video tutoriales, lecciones en archivos, tareas y devoluciones, estará enmarcado en el método activo de autoaprendizaje, desarrollando situaciones reales centradas en las actividades del sujeto que aprende, efectuando la recuperación de saberes previos, el análisis, la reconstrucción y la evaluación de los contenidos propuestos y creación de nuevos conocimientos.

El aprendizaje será por procesos incluyendo de manera sumativa, autoevaluación, participación activa entre pares, con el Profesor Tutor y por medio de las vías y medios de comunicación de la plataforma.

8. Estrategias de evaluación

La calificación obtenida se corresponde a la suma de aciertos respecto del total del puntaje correspondiente. En este módulo, la ponderación total es del 100%, siendo la calificación mínima de aprobación, el 70%.

8.1. Tabla de sistema de evaluación

Instrumentos de evaluación	Contribución a la calificación
Participación en foros	15%
Control de lecturas	15%
Entrega de trabajos	30%
Evaluación final	40%
Total	**100%**

8.2. Rúbrica del módulo

Estándares de Aprendizaje	Incipiente	En Proceso	Bueno	Excelente
Participación en foros	Utiliza el foro mínimamente. Se limita a realizar las actividades solicitadas.	Utiliza el foro suficientemente. Realiza las actividades solicitadas y escribe comentarios.	Utiliza el foro claramente. Realiza las actividades solicitadas, comenta, aporta y consulta.	Utiliza el foro activamente. Establece un relacionamiento, propicia el diálogo/debate.
Control de Acceso – Credenciales	Conoce mínimamente los conceptos del Control de Acceso y Credenciales	Conoce suficientemente los conceptos del Control de Acceso y Credenciales	Conoce claramente los conceptos del Control de Acceso y Credenciales	Conoce perfectamente los conceptos del Control de Acceso y Credenciales
Correo Electrónico	Conoce mínimamente los conceptos de Correo Electrónico.	Conoce suficientemente los conceptos de Correo Electrónico.	Conoce claramente los conceptos de Correo Electrónico.	Conoce perfectamente los conceptos de Correo Electrónico.
Ingeniería Social	Conoce la técnica básica del programa. Necesita ayuda para aplicar una técnica.	Conoce suficientemente la técnica del programa. Necesita ayuda con las funcionalidades.	Conoce bien la técnica y aplica las buenas prácticas del programa.	Conoce perfectamente las técnicas de buenas prácticas y utiliza todas sus funcionalidades.
Navegación Segura	Conoce el funcionamiento básico de algunos de los programas de Navegación.	Conoce suficientemente algunos programas de Navegación.	Utiliza suficientemente varios programas de Navegación.	Utiliza y combina varios programas de Navegación.

Seguridad en Equipos	Conoce el funcionamiento básico de Seguridad en equipos. Necesita ayuda para comprender el contenido.	Entiende suficientemente el funcionamiento de Seguridad en equipos.	Utiliza eficientemente los conceptos de Seguridad en equipos.	Utiliza y aplica eficientemente las técnicas y buenas prácticas sobre Seguridad en equipos..
Protección de los Datos	Conoce mínimamente los conceptos de Protección de Datos.	Conoce suficientemente los conceptos de Protección de Datos.	Conoce claramente los conceptos de Protección de Datos.	Conoce perfectamente los conceptos de Protección de Datos.

9. Público objetivo

Este curso está dirigido a ciudadanos interesados en conocer las amenazas más comunes existentes en el mundo digital, y las medidas de protección. No requiere conocimientos técnicos y no posee ningún pre-requisito

10. Requisitos recomendados

Participar de este módulo requiere de una conexión a Internet suficiente para visualizar vídeos, ya que una parte de los contenidos ofrecidos se encuentra en este formato. Es necesaria cierta habilidad en el uso de entornos digitales para la realización de actividades que facilitarán la reflexión.